American Journal of Computer Science and Technology
2022; 5(2): 49-55
http://www.sciencepublishinggroup.com/j/ajcst
doi: 10.11648/j.ajcst.20220502.14
ISSN: 2640-0111 (Print); ISSN: 2640-012X (Online)

Research on Information Security and Privacy Technology Based on Blockchain

Zhong Ke, Tuyatsetseg Badarch[*]

Department of Information Technology, School of Information Technology and Design, Mongolian National University, Ulaanbaatar, Mongolia

Email address:
ba.tuyatsetseg@mnun.edu.mn (T. Badarch)
[*]Corresponding author

To cite this article:
Zhong Ke, Tuyatsetseg Badarch. Research on Information Security and Privacy Technology Based on Blockchain. *American Journal of Computer Science and Technology*. Special Issue: *Advances in Computer Science and Future Technology*. Vol. 5, No. 2, 2022, pp. 49-55. doi: 10.11648/j.ajcst.20220502.14

Received: March 28, 2022; **Accepted**: April 15, 2022; **Published**: May 24, 2022

Abstract: Blockchain provides IoT security and privacy in all industries including manufacturing, finance, healthcare, supply chain, e-governance, education, banking, and trading through decentralization, persistency, anonymity, and auditability characteristics. This paper presents the blockchain technology assimilating with other data security technologies to design a blockchain based data sharing system. Based on the design the network architecture of data sharing system, we test and analyze various processes in data sharing. To test the function and security of the system, we have built a test environment with data sharing system consisting of three blockchain nodes, four data participant nodes (three data users, one data provider), and a data-sharing system composed of CA. We developed Base App as an application provided by the data user, including addition, deletion, check modification of data in the application code for data sharing. We simulated an experiment related scenario, and then we wrote a program to generate the vehicle information data and import it into MySQL for storage. The paper has found some valuable results of functional test, system test, safety test, and performance test of the data sharing system. This system realizes the possibility of a system that can connect multiple participants and their corresponding data.

Keywords: Blockchain, Data Sharing, Data Security, Data Privacy, Information Security

1. Introduction

The concept of blockchain was originally introduced by scholars under the allies “Satoshi Nakamoto”. It was originally set out to be a point-to-point decentralized, antitrust based trading system based on cryptography technology with distributed storage in a distributed storage. As an emerging technology, although blockchain is currently experiencing a lack of a deep research to guide studies in the field, blockchain technology has successfully penetrated into economic transaction systems in organizations, and has the potential to revamp heterogeneous models in different industries [1].

As an example, a particular study may overlap two areas of blockchain algorithm and blockchain data security. The research shows valuable results of blockchain framework that provides the blockchain taxonomy, blockchain consensus algorithms, blockchain applications, technical challenges, and recent advances in tackling the challenges [2].

At this early stage of the blockchain technology development, it was not be clear as to what category, meta data, meta technology, however, the current studies provide a theme called ‘blockchain data security and privacy’ including subcategories such as blockchain security, blockchain data sharing. The privacy and security problems are always associated with storing and sharing personal data [2]. Security of data sharing has been addressed by security techniques as well as experimental approaches, for example, carrying out information without trusting anybody and possibly replacing the centralized controlling authority. All these problems including security, privacy, user transparency and control, and incentives for data sharing can be solved efficiently based on blockchain.

2. Research Background

Blockchain has numerous benefits such as decentralization, persistency, anonymity, and auditability for cryptocurrency technology, financial services, risk management, internet of things (IoT), and various services [2]. Based on the above unique characteristics, blockchain technology is becoming a valuable technology for the next generation of internet interaction systems, smart contracts, public services, Internet of Things (IoT), reputation systems, and security services [2-7].

It also includes neat functions like chronological storage, ensuring an impossible situation for forgers to duplicate original product by using cryptography. Each node saves a copy of the chain to ensure data transparency [8]. This technology has attracted the attention of governments, major enterprises, and the scientific community. It is also developing rapidly, for instance, there has been a multitude of cryptocurrencies in the market. Bitcoin represented the first generation of blockchain technology by using it to successfully record transactions in all digital currencies. Soon after came Ethereum with the added improvement of smart contracts [9]. Alike cryptocurrencies, blockchain technology has also been evolving in many sectors such as intellectual property, logistic records, food safety, health care, networks, data security [9-13]. The technology promises a securely distributed framework to facilitate sharing, exchanging, and integration of information across all users and third parties.

It is essential for the planners and decision makers to analyze it blockchain in depth for its suitability in various industries and business applications [1].

In the process of data sharing, blockchain can effectively solve the problem of data privilege [13]. Data privilege means how to know who has what right to access the given data. Before cloud computing, most business models and computing models were their machines, processing their data. After cloud computing, people began to rely on putting their data in other people's machines. The problem with this protocol is that there is no way of knowing the machine is doing what we want it to. This is a break of data privilege thus breaking the data's integrity.

Data sharing is inevitable to the further development of society. People are constantly exploring the idea of a data-sharing system based on blockchain and data security technology to solve problems like data ownership [7]. This paper looks into developing data security through blockchain technology and designs a data-sharing system.

3. Analysis of Security and Privacy Characteristics of Blockchain

Blockchain has attracted great attention in many sectors including the architecture, engineering, construction, and operation industry [14]. Blockchain has been widely paid attention mainly because of the following characteristics for data sharing field:

(1) Out of centralization. There is no center to the transmission of data. It uses the distributed system to complete the data sharing and storage. Under this mechanism, attacking a certain node in the system is not sufficient to affect the entire blockchain network.

(2) Transmission. Blockchain exposes data recording and updates operations to the whole network nodes. As a distributed technology, the programs, rules, and node access methods running on the network to exchange data are all open.

(3) Autonomy. The environment in which all nodes in a blockchain network exchange data with each other is distrust. This is because blockchain adopts specific consensus algorithms, so trust in "people" becomes trust in the machine.

(4) Unchangeable information. With blockchain, information cannot be changed. The essence of it is having decentralized and distributed databases where each node holds a copy of the data for data sharing situation. Data consistency is maintained by the consensus of most nodes. Therefore, when a blockchain network reaches a certain scale the degree of dispersion reaches a certain scale. All of these technical terms mean that the network is not managed by humans in the data exchange, thus preventing data tampering.

(5) Anonymity. With the help of blockchain technology, the data exchange and transactions can be completed anonymously. Data exchange/sharing between nodes is completed by a fixed and predicted algorithm based on the address rather than personal identity [15].

A consensus algorithm is the basis for the normal operation of blockchain and ensures the above characteristics. It is the algorithm that blockchain nodes can reach an agreement on transactions and generate new blocks. It is also the core algorithm of blockchain.

On the premise of ensuring the above characteristics, the combination of smart contracts and blockchain enables blockchain to be applied to more fields. Smart contracts are a set of protocols that can automatically execute certain tasks. It is similar to paper contracts. It builds a program contract with readable nodes in the blockchain system. Some characteristics of the blockchain also provide support for the realization of smart contracts on the blockchain [3]. Users can write specific smart contracts for specific business needs, and provide users with a call interface. Smart contracts complete the transaction and save the information to the blockchain.

4. Methodology of Data Sharing Design Based on Blockchain

We design the network architecture of data sharing system in combination with traditional data sharing solutions. After we introduce the network topology of the whole system and describe the components and functions of the system.

4.1. Traditional Centralized Architecture of the Data Sharing System

A centralized architecture implies the availability of a single or a few entities that have control over the entire network. From a security point of view, this single centralized entity needs to monitor the safety of the entire network.

The centralized architecture of the IoT system provides a good start for connecting a wide range of various objects and devices all over the world under the responsibility of a centralized server which manages and control all communication between devices and provides the required identification and authentication for different devices and objects. However, it is unable to support large-scale IoT networks which need to be extended in the near future especially with the huge increase of adopting IoT solutions [16-17].

Figure 1 shows the traditional centralized data sharing system architecture that requires the help of a trusted third party. The centralized server also provides the directory services and the data sharing services externally. All participants added to the data-sharing system are registered on the third-party server to complete identity authentication. The data provider stores data and relevant permissions into the centralized server and writes metadata-related information describing the directory of the centralized data. The directory is visible to all participants, asking which participants can join the data-sharing system and learn the relevant information related to the data through metadata information.

4.2. Distributed Architecture of the Data Sharing System

To solve the problems existing in the centralized data sharing system, we improve the architecture and propose a distributed data sharing system. In our system, CA is used to issue certificates for identity authentication and safe communication between nodes. *It* realizes the discovery of participants through blockchain and realizes data confirmation through the attribution of data records. In addition, each participant needs to install data-sharing platform software on its nodes to join the system, forming a P2P network between the participants. The data will not leave the node of the data provider, all sharing operations are completed on the nodes of the data provider to protect the security of the data.

Figure 2 describes the network architecture of the data-sharing system here, which consists of three parts: CA, a blockchain platform, and a data-sharing platform.

Furthermore, we design the system software architecture, including the system software composition, the functions of the various modules, and the relationship between the modules. Figure 3 shows the overall architecture of the system software, which consists of two parts: the data-sharing platform software and the blockchain system.

4.3. Data Sharing Contracts

We use data sharing contracts as electronic contracts to support data sharing applications. We chose xChain, the blockchain basic platform independently designed and implemented by our laboratory, to build the blockchain part of the data-sharing system. xChain belongs to the affiliate chain and is divided into the network layer, data layer, core layer, and application layer.

In the basic architecture of the xChain system, the network layer is responsible for maintaining the topology of the entire network and realizing the communication among the blockchain nodes.

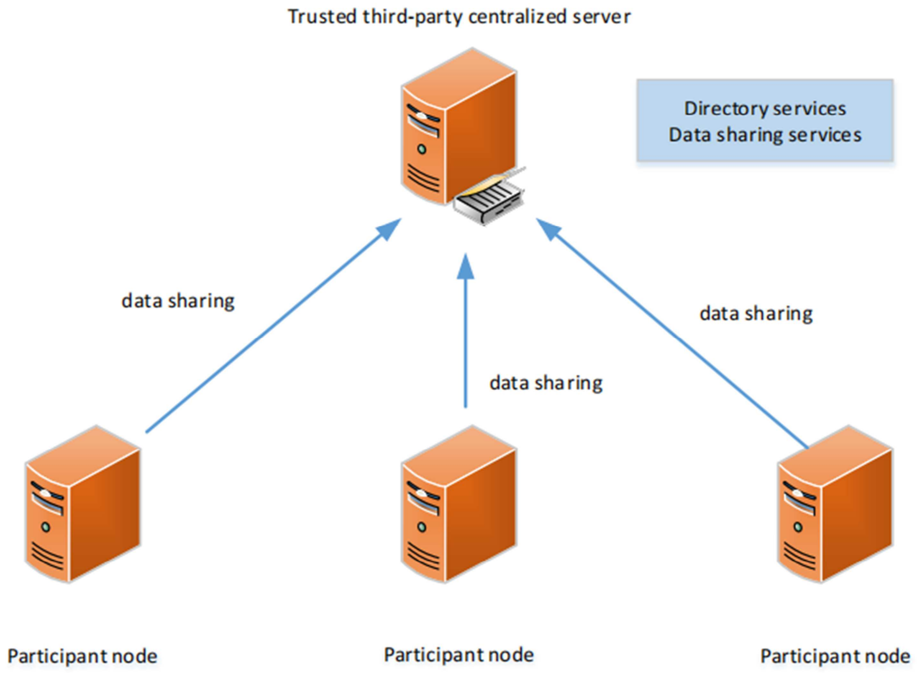

***Figure 1.** Centralized data-sharing system network architecture.*

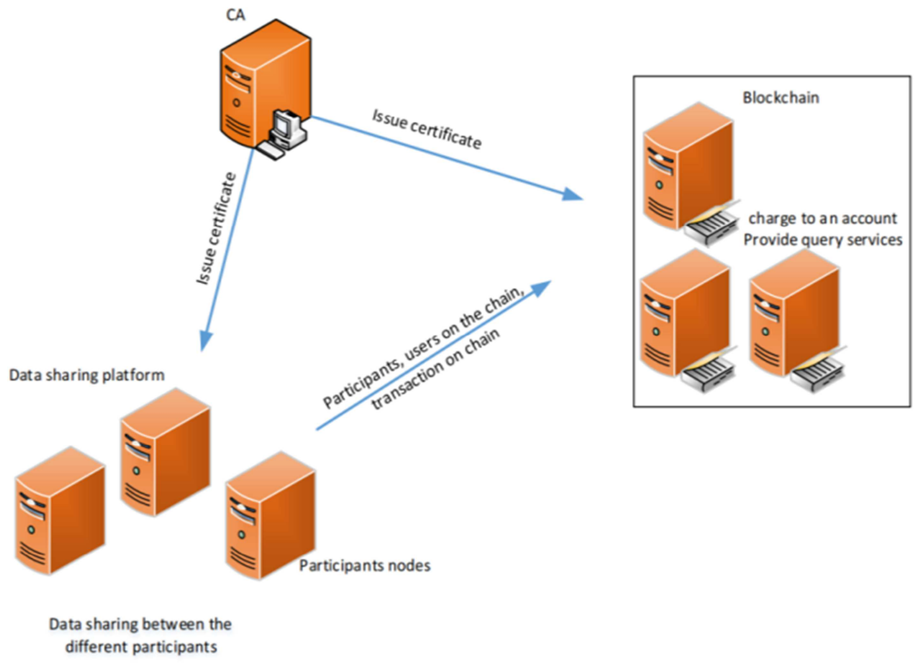

Figure 2. *Data-sharing system network architecture.*

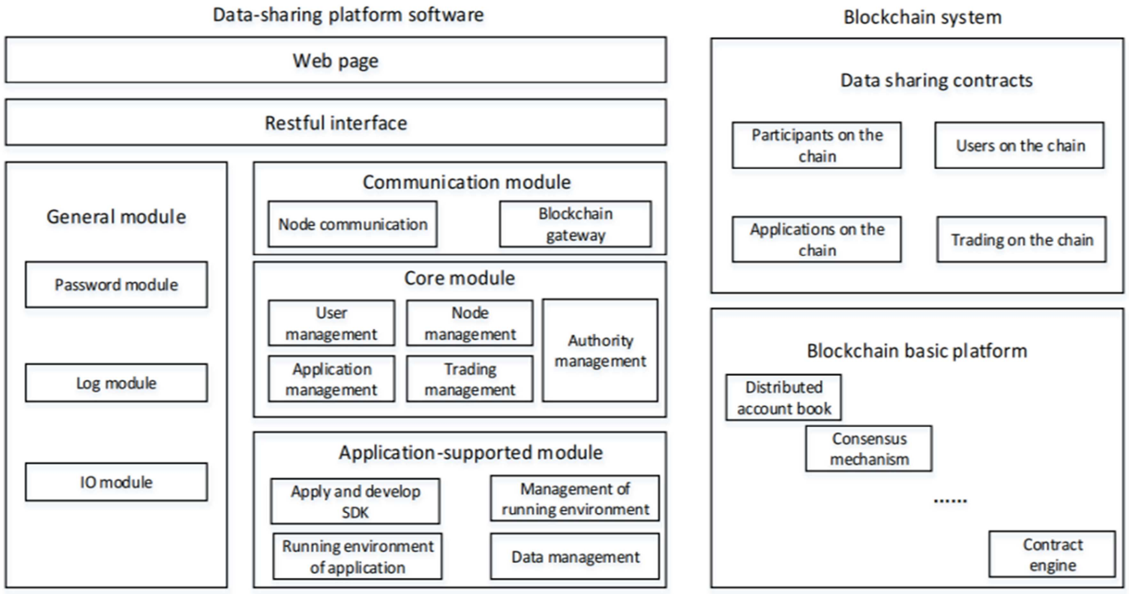

Figure 3. *System software architecture.*

5. On Some Results of Data Sharing Security and Privacy Test Based on Blockchain

5.1. System Test and Analysis

First, the process of building the required environment is introduced. After the former process, we test and analyze various processes in data sharing. To test the function and security of the system, we have built a test environment with data sharing system consisting of three blockchain nodes, four data participant nodes (three data users, one data provider), and a data-sharing system composed of CA (Table 1).

Table 1. *Testing environment.*

Hardware	CPU	Intel i5-8400, 2.8.GHZ*6
	Internal storage	8 GB
	Network	Downside bandwidth 60Mbps, Up bandwidth 30Mbps
Software	Operating system	Ubuntu 16.04
	Docker	Version 17.05
	Database	MySQL Version 5.7.25

We simulated an experiment related scenario, and then we wrote a program to generate the vehicle information data and import it into MySQL for storage. After building all parts of the system, the data sharing contract is deployed to each node of the blockchain as an application related to the upper-level data-sharing business of the blockchain. To test the system, we developed Base App as an application provided by the data user, including addition, deletion, check modification of data in the application code for data sharing. Furthermore, to automate testing, test scripts will be developed using a programming and the system will be tested using the robot framework.

5.2. Function Tests

Functional tests verify that the system operates as expected when a specific operation is performed. We further subdivided the functional tests into four parts: initialization-related function tests, application deployment function testing, application subscription function testing, and application call function testing. Among them, the initialization related function test includes the test of the participant node initialization and the user-related registration, login, authorization, and other aspects (Table 2).

The results of relevant functional tests during the initialization phase are shown below (Table 2).

Table 2. *Relevant functional tests during the initialization phase.*

	Case description	Excepted results	Results
1	Root users shall log in and input the submitted participating node information.	Started successfully, and successfully wrote the root users and participant information on the blockchain	Yes
2	User make registration operation, the root user approval passed	Register successfully, with user-related information on the chain	Yes
3	Root user authorizes an ordinary user to become an administrator user	Operate successfully, the user role on the chain changed	Yes
4	Administrator user, root user log off the ordinary user	Operate successfully, the user status on the chain is log-out	Yes
5	Users view their own relevant information	Operate successfully	Yes
6	The Administrator user approves the registration request	Register successfully, user information is saved on the chain	Yes
7	Root undoes the administrator user	Operate successfully, the user role changes on the chain	Yes
8	Ordinary users view the information and registration requests of other users	Operation failed, no permission	Yes
9	Ordinary users view the data-sharing transactions	Operation failed, no permission	Yes
10	Users view the data provider and user information on the chain	Operate successfully	Yes
11	Administrator users, root users add policies to the relevant access control list	Operate successfully	Yes
12	Ordinary users add records to the access control list	Operation failed	Yes

The results of functional tests about the application deployment are shown below (Table 3).

Table 3. *Functional tests of the application deployment.*

	Case description	Excepted results	Results
1	The data user initiates a deployment request and the user administrator user approves	The operation was successful with an application deployment request on the chain received by the data provider	Yes
2	The data provider administrator obtains the request user certificate from the chain, validates the signature, and downloads the application	Verify the signature through, the application after the download decryption success	Yes
3	The data provider approves the subscription request	Generate a docker mirror that chain the application deployment transaction updates	Yes
4	Applications approved by users through the blockchain query	Operate successfully	Yes
5	The data user administrator denied the deployment request	Deployment failed with the corresponding transactions on the chain	Yes
6	The data provider administrator denied the deployment request	Deployment failed with the corresponding transactions on the chain	Yes
7	The user requesting the deployment application imported an invalid target participant ID	Deployment failed	Yes
8	The user sends an invalid App ID deployment request to the provider	Deployment failed	Yes
9	The user sends an invalid user ID deployment request to the provider	Deployment failed	Yes
10	Add a user ID to the deployment access control list to allow specific users to deploy the application	There is no manual audit, the corresponding user request audit passed, there are corresponding records on the chain, the audit user and the added policy users match	Yes
11	Add a user role to the deployment access control list to allow administrators to deploy the application	The administrator deployment request is passed without audit, the ordinary user request is saved and waiting for audit, and the audit user matches the added policy user	Yes
12	Add a target participant ID to the deployment access control list to allow the deployment of applications	The deployment request sent to the participant need not be manually reviewed and the audit user matches the added policy user	Yes
13	Add the participant's ID, IP to the deployment access control list to allow it to deploy the application	The requests of the corresponding participants need not be reviewed manually, and the audit user matches the added policy user	Yes
14	Change the decision result to negative decisions for the use cases related to the access control list	All requests are denied and the audit user matches the Add policy user	Yes
15	Application deployment records on the user query chain	The query was successful	Yes

The results of functional tests about application calling are shown below (Table 4).

Table 4. *Functional tests of application calling.*

	Case description	Excepted results	Results
1	Users who do not subscribe to the application initiate a call request, using randomly generated trigger credentials.	Call failed	Yes
2	The subscription ID in the call request from the user does not match the trigger credentials	Call failed	Yes
3	The user sends a non-existent call ID to the provider	Call failed	Yes
4	Add a database to the database access control list	Access to the database was denied	Yes
5	Add a database, table name to the database access control list	Access to the table was denied	Yes
6	Add a database, a table name, and a data table field to the database access control list	Access to these fields was denied	Yes
7	Add an action type to the database access control list	The corresponding operation is rejected	Yes
8	Add the user ID and the user roles to the database access control list, respectively	The corresponding request is denied to the database while calling the application	Yes
9	Add a participant to the database access control list	Access request from the corresponding participating user is denied	Yes

5.3. Safety Test

We design safety test cases to verify the system security from several aspects of sensitive data encryption, identity authentication, access control, and isolation environment computing. As it is shown in Table 5.

Table 5. *Safety test cases.*

	Case description	Excepted results	Results
1	Replace the participant certificate, and the new certificate is not issued by the CA	No authentication and cannot establish secure communication	Yes
2	Replace the certificate of the blockchain node, the new certificate is not issued by the CA	No authentication and cannot establish secure communication	Yes
3	Modify the communication data during the communication process	Digital signature validation has failed and cannot communicate	Yes
4	For requests initiated by a specific user, use the private key signature of another user	Signature validation has failed, and the request is invalid	Yes
5	During publishing the application, replace the application after calculating the hash	The application hash does not match the chain hash and the deployment request is invalid	Yes
6	For applications and credentials of encryption storage, a key solution that does not match the encryption key is used	decrypt failed	Yes
7	Users who have failed the audit log in	log failed	Yes
8	Send various requests to the participant node for the audited user	Operate failed	Yes
9	Ordinary users log in to obtain the application deployment, subscription requests	Operate failed, no permission	Yes
10	The ordinary user reviews a deployment request	Operate failed, no permission	Yes
11	The ordinary user audit passes a subscription request	Operate failed, no permission	Yes
12	Ordinary users add records to each access control list	Operate failed	Yes
13	Applications running in the container begin modifying the system files	The host system files are not affected, and the remaining applications in the containers are operating normally	Yes
14	The host process tries not to communicate with the in-container process through the port that the executor listens to	Unable to communicate	Yes

5.4. Performance Test

In performance testing, we test the throughput of a data provided by calling an application continuously. Then, 3 different data users continuously call 3 applications at the same time. We analyzed 15 sets of data and the results are shown in Table 6.

The throughput of a single user calling an application is around 240 and higher when three users call concurrently. Since the process requires for it to reach a consensus between the blockchain nodes, it takes some time. The throughput is smaller than a centralized system.

Table 6. *Performance testing results.*

Requesting times	Categories	Throughput
10000	A user calls an application	236
	Three users call three applications concurrently	614
20000	A user calls an application	241
	Three users call three applications concurrently	603

6. Conclusion

In this research, we study a blockchain based data security technologies. We design and testing the data sharing system based on blockchain. We have found some valuable results shown in the testing results including functional test, system test, safety test, as well as performance test. This system realizes the possibility of a system that can connect multiple participants and their corresponding data. In future, we plan to extend the tests to cover other elements of the data sharing system based on block chain.

References

[1] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and C. Yang, "The blockchain as a decentralized security framework," IEEE Consum. Electron. Mag., vol. 7, pp. 18-21, 2018.

[2] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," International Journal of Web and Grid Services, vol. 14, pp. 352-375, 2018.

[3] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in 2016 IEEE symposium on security and privacy (SP), 2016, pp. 839-858.

[4] B. W. Akins, J. L. Chapman, and J. M. Gordon, "A whole new world: Income tax considerations of the Bitcoin economy," Pitt. Tax Rev., vol. 12, p. 25, 2014.

[5] Y. Zhang and J. Wen, "An IoT electric business model based on the protocol of bitcoin," in Intelligence in Next Generation Networks (ICIN), 2015 18th International Conference on, 2015, pp. 184-191.

[6] M. Sharples and J. Domingue, "The blockchain and kudos: A distributed system for educational record, reputation and reward," in European Conference on Technology Enhanced Learning, 2016, pp. 490-496.

[7] C. Noyes, "Bitav: Fast anti-malware by distributed blockchain consensus and feedforward scanning," arXiv preprint arXiv: 1601.01405, 2016.

[8] Q. Xia, E. B. Sifah, K. O. Asamoah, et al. Me DShare: Trust-less Medical Data Sharing Among Cloud Service Providers Via Blockchain. IEEE Access, 2017, 5: 14757-14767.

[9] V. Patel. A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. Health Informatics Journal, 2018, 25 (4): 1398-1411.

[10] X. Liang, J. Zhao, S. Shetty, et al. Integrating Blockchain for Data Sharing and Collaboration in Mobile Healthcare Applications. 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Montreal, 2017.

[11] H. Ruhua, C. Chuang. Study on the Sharing Cooperation Mode of U.S. Open Government Data. Library & Information Service, 2016.

[12] M. Benchoufi, P. Ravaud. Blockchain technology for improving clinical research quality. Trials, 2017, 18 (1): 335.

[13] W. T. Li, S. Andreina, J. M. Bohli, et al. Securing Proof-of-Stake Blockchain Protocols. Data Privacy Management, Cryptocurrencies and Blockchain Technology, Oslo, 2017, 297-315.

[14] Farhad Daneshgar, Omid Ameri Sianaki, Prabhat Guruwacharya, Blockchain: A Research Framework for Data Security and Privacy.

[15] Szabo, N. (1997). Formalizing and securing relationships on public networks. First Monday 2. doi: 10.5210/fm.v2i9.548.

[16] Dolog, P., and Vassileva, J. (2005). “Decentralized, agent based, and social approaches to user modeling (DASUM),” in Workshop DASUM-05, at the 9th International Conference on User Modeling (UM'05) (Edinburgh).

[17] Thilakarathna, K., Petander, H., Mestre, J., and Seneviratne, A. (2014). MobiTribe: cost efficient distributed user generated content sharing on smartphones. IEEE Trans. Mobile Computing. 13, 2058–2070.